

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF
THE VEHICLE DESCRIBED AS: 2019 Silver
Nissan Pathfinder, VIN
5N1DR2MN9KC643033, Further Described in
Attachment A.

Case No. 3:21-sw-19

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT
TO SEARCH AND SEIZE**

I, Melvin Gonzalez, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of a 2019 Silver Nissan Pathfinder, (hereinafter referred to as "VEHICLE") as further described in Attachment A, and for the seizure from the VEHICLE of items as further described in Attachment B.
2. I am a Special Agent with the Federal Bureau of Investigation and have been so employed by the FBI for over fifteen years. I am currently assigned to the Richmond Field Office, Richmond, VA. I am assigned to the Child Exploitation Task Force, which conducts investigations related to child sex trafficking, child pornography, child abductions and other crimes against children. I have received training from the FBI in the areas of child exploitation. I was previously assigned for six years to the San Juan Field Office, where I investigated violent crimes, gangs, drug trafficking and other matters unrelated to crimes against children.
3. In the course of my employment as a sworn law-enforcement officer, I have participated in the execution of numerous search warrants resulting in the seizure of computers, magnetic

storage media for computers, other electronic media, and other items evidencing violations of state and federal laws, including various sections of Title 18 of the United States Code, including § 2251, involving production of child pornography, § 2252A, involving a variety of child exploitation and child pornography offenses, and § 2422, involving online enticement or coercion of a minor to engage in illegal sexual activity.

4. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.
5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence and instrumentalities Attempted Coercion and Enticement of a Child, in violation of 18 U.S.C. § 2422(b) and Travel With Intent To Engage in Illicit Sexual Conduct with a Child, in violation of 18 U.S.C. § 2423(b) are located in the VEHICLE described in Attachment A. There is also probable cause to search the VEHICLE described in Attachment A for evidence and instrumentalities of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). Specifically, the Court is “a district court of the United States ... that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

RELEVANT STATUTORY PROVISIONS

7. **Attempted Coercion and Enticement:** 18 U.S.C. § 2422(b) provides that whoever, using the mail or any facility or means of interstate or foreign commerce, knowingly persuades,

induces, entices, or coerces any individual who has not attained the age of 18 years to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be imprisoned not less than 10 years or for life.

8. **Travel with Intent To Engage in Illicit Sexual Conduct:** 18 U.S.C. § 2423(b) provides that a person who travels in interstate commerce ... with a motivating purpose of engaging in any illicit sexual conduct with another person shall be fined under this title or imprisoned not more than 30 years, or both.
9. **Illicit Sexual Conduct:** 18 U.S.C. § 2423(f)(1) defines “illicit sexual conduct” to include a sexual act (as defined in section 2246) with a person under 18 years of age that would be in violation of chapter 109A if the sexual act occurred in the special maritime and territorial jurisdiction of the United States.

TECHNICAL TERMS

10. Based on my training and experience, I use the following technical terms to convey the following meanings:
 - a. **“Computer,”** as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”
 - b. **“Computer Server” or “Server,”** as used herein is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user’s computer via the Internet. A domain name system (“DNS”) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her

web browser. Essentially, the domain name must be translated into an Internet Protocol (“IP”) address so the computer hosting the web site may be located, and the DNS server provides this function.

- c. **“Computer hardware,”** as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).
- d. **“Computer software,”** as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- e. **Wireless telephone:** A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities

include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. **Digital camera:** A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- g. **Portable media player:** A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- h. **GPS:** A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation

devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- i. **PDA:** A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- j. **Tablet:** A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, which is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks,

802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

- k. The “**Internet**” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- l. “**Internet Service Providers**” (“**ISPs**”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (“**DSL**”) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an “e-mail address,” an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider (“**ISP**”) over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.
- m. “**Internet Protocol address**” or “**IP address**” refers to a unique number used by a computer to access the Internet. An IP address is a series of four numbers, each in the range 0-255,

separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- n. “The terms **“records,” “documents,”** and **“materials,”** as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (“DVDs”), Personal Digital Assistants (“PDAs”), Multi Media Cards (“MMCs”), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
- o. **“Website”** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (“HTML”) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (“HTTP”).

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

11. As described above and in Attachment B, this application seeks permission to search for records that might be found on electronic devices including cellular phones, in whatever form they are found. The warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).
12. *Probable cause.* I submit that there is probable cause to believe records will be stored on electronic devices including cellular phones, for at least the following reasons:
 - a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Depending on a variety of factors, a particular computer could easily not overwrite deleted files with new data for many months, and in certain cases conceivably ever.
 - b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

13. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the electronic devices including cell phones because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the

attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.
- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

14. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

15. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of electronic devices including cellular phones consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

PROBABLE CAUSE

- 16. On or about June 23, 2020, as part of the FBI Richmond CETF, an online covert employee (OCE) used a covert social media account to target subjects willing to travel to the Richmond, Virginia area to engage in sexual conduct with a minor. The OCE set up a profile posing as an adult intermediary who had access to both a male and a female minor.
- 17. The OCE posted a profile on an online platform and subsequently responded to subjects who indicated a desire to meet with minors.

18. The OCE posted an undercover (UC) profile on "Alt.com." Alt.com is an online network for members interested in alternative forms of sexual relationships and friendship. Users can bond over fetishes, kinks, and BDSM (Bondage, Discipline, Sadism, and Masochism), as well as explore the site's large stockpile of sexual videos, articles, and other content. The UC profile noted that the user was an adult female from Chesterfield, Virginia. It also included a list of kinks to include "Daddy/babygirl", "mom/son", "young/old," "Mommy/Daddy play" and "taboo family".

19. On August 16, 2020, an individual utilizing the username "LordWhisper" contacted the OCE through the UC profile, (hereinafter referred to as "UC Mom" to protect the integrity of the OCE online profile), on Alt.com. LordWhisper sent the following messages:

LordWhisper: Hello there are you still looking for someone have you found someone to enjoy I'm very discreet and interested

LordWhisper: Whats your limits and breast size

20. The following messages were exchanged between LordWhisper and UC Mom on August 16, 2020 and August 17, 2020:

LordWhisper: Hi there , have u found anyone yet

UC Mom: I've talked to since interesting people
What about you?

LordWhisper: I have as well most are fakes and liars I'm seeking real and someone that wants the lifestyle not play at it
How many kids do you have

UC Mom: I have two
Do you have any kids?

LordWhisper: One 26 yr daughter , how old are yours , are you on bc you can breed
I'm a daddy Dom as well

UC Mom: Mine are still young
I'm not on bc and I can breed

LordWhisper: Mmmmmm do I want more , love to seed you , what ur limits and off limits

LordWhisper: Are you breastfeeding

LordWhisper: I would like to

UC Mom: I'm not into blood or pee

UC Mom: Everything else is ok

UC Mom: What about you?

LordWhisper: Ok with hose and will respect them I really don't have any limits , I like lots of things kinky naughty and taboo

LordWhisper: Are you interested in only locals

UC Mom: No I'm open to travel and long weekends

LordWhisper: Are you into taboo

LordWhisper: I'm really looking for someone to enjoy and explore, I lost my sun and her 6 yr old daughter 3 years ago to a bad car wreck , so starting to look now

LordWhisper: Do you like k9

21. LordWhisper then sent an image of what appeared to be a middle-aged white male wearing an orange shirt and claimed that he was the individual in the image. He asked the OCE, acting as UC Mom, if she had a Kik account. The OCE provided the Kik username for UC Mom, and LordWhisper provided his Kik username, "w1ldncrazy1". LordWhisper's Alt profile stated he is a 55-year-old male with a date of birth (DOB) of February 20, 1965 who lives in the Florence, South Carolina area.

Also on August 17, 2020, the OCE received the following messages on Kik from an individual with the username "w1ldncrazy1", which LordWhisper previously indicated as his Kik username:

w1ldncrazy1: Hello from lordwhisper

UC Mom: Hi

w1ldncrazy1: Are you currently seeing someone or involved with a Dom tell me more about yourself

please feel free to ask me any question

w1ldncrazy1: If we decide I have no issues driving up for meeting to see if we hit it off

UC Mom: I'm not currently seeing anyone
It's just been me and my kids since my husband died

22. Later in the conversation, the following exchange occurred after w1ldncrazy1 asked the OCE acting as UC Mom to tell him more about herself:

UC Mom: I'm 39 with two children, a 10 yr old girl (hereinafter referred to as "UC Girl") and an 8 yr old boy (hereinafter referred to as UC Boy)
I work and hate people who are lazy
I'm looking for a man to take my husbands place as the head of our family
UC Mom: What are you looking for?

w1ldncrazy1: I'm searching for a female that is in the lifestyle that is willing and understands what the lifestyle is about that wants to enjoy it together and explore it together someone that wants me for me as I told you I am a daddy Dom Im very nurturing and caring but stern and strict , I have no problem that you have kids, do you hide the lifestyle from them of who I are

w1ldncrazy1: Nice ages ,

w1ldncrazy1: I'm looking for honest and loyalty

UC Mom: My kids are in the life
If that's a problem I totally get it

w1ldncrazy1: I'm ok with that , Im.lookinh for that

23. The OCE, acting as UC Mom, indicated that her daughter, UC Girl, had previously engaged in sex acts with her and her husband, who purportedly passed away approximately two years ago. w1ldncrazy1 then disclosed a previous relationship with an unknown female named "Lisa" and her minor daughter. The following conversation occurred in reference to that relationship:

UC Mom: Her daughter serviced you?

w1ldncrazy1: Yes

UC Mom: Wonderful
How old was she?

w1ldncrazy1: They both did started at 4

UC Mom: She was 4???

Amazing

w1ldncrazy1: On her 5th bday mom held her legs apart

w1ldncrazy1: Mom always sucked my dick in front of her no matter what and I would also f*** mom in front of her and she asked could she taste and try one day

w1ldncrazy1: Daddy dick is hard

UC Mom: What did you do to her?

24. The communication between the OCE and w1ldncrazy1 continued, and the following exchange then occurred in reference to UC Mom's eight year old son:

w1ldncrazy1: I will for sure

UC Mom: Will what?

w1ldncrazy1: Finger his ass

w1ldncrazy1: And you two as well

UC Mom: You don't mind his age or him being a boy?

w1ldncrazy1: Not at all

UC Mom: Good

w1ldncrazy1: Work his ass till he can take Daddy's cock

UC Mom: Oh wow

You're nasty

w1ldncrazy1: You can suck on him as he sits down on Daddy dick

25. Later, the conversation also referenced UC Mom's 10 year old daughter and included plans to travel to Virginia and engage in sexual activity with the UC Mom and both minor children at the same time:

w1ldncrazy1: Then you can decide whether you would like to continue and go further

UC Mom: What would be further?

w1ldncrazy1: And yes they would hear you scream and cry as Daddy was fucking you

w1ldncrazy1: Meeting the kids

w1ldncrazy1: Daddy's going to fuck you from behind as you suck on his little dick and lick her tight little pussy

26. wlldncrazy1 stated he would enjoy having a taboo family, and that he lives just over the South Carolina border and would be willing to drive to the Richmond, Virginia area to meet the OCE. He also sent a video of what appears to be a white male masturbating and ejaculating.

27. From approximately August 19, 2020 to approximately January 8, 2021 the OCE and wlldncrazy1 engaged in sporadic conversation. On January 8, 2021 the following exchange occurred:

UC Mom: I accidentally logged out and lost our messages
Can you catch me up?

wlldncrazy1: I'm a daddy Dom , I'm 56 today matter of fact
wlldncrazy1: You live in va correct

UC Mom: I do
Happy birthday!!!!
Any big plans?
And what's your name?

wlldncrazy1: Dave none at all , and ty , like to have my girls for my bday

28. wlldncrazy1 stated he lives close to Dillon, South Carolina, and is approximately four hours away from Richmond, Virginia. He also stated he works in computers. Later in the conversation, the following exchange occurred in reference to UC Mom's minor son, as well as previous sexual encounters wlldncrazy1 had with a minor:

wlldncrazy1: I'm not by but I would enjoy him sucking my dick and mentoring him on dominating you too

wlldncrazy1: And depending on the dynamic and how things go I might just bend him over and take him once or twice

wlldncrazy1: I really enjoyed sitting on the couch and her head bobbing up and down on my dick as Mom played with her pussy getting it all warm and wet and juicy and she would climb up on Daddy and bounce up and down and ride it taking it to the deepest point that she would crying but wanting more

wlldncrazy1: I so enjoyed her buddy and breast

Later in the same conversation, the following then took place:

wlldncrazy1: Too bad you don't go into his room right now and pull his little panties off to one side and slide your finger up his crack feeling his little hole and massage in it in and out not getting your finger too deep at all but just rubbing his little hole

UC Mom: I like how nasty you are that you want me to fuck with UC Boy instead of UC Girl

wlldncrazy1: Oh I want you to fuck with both of them but I think you would enjoy sliding that finger up his crack if you pull his panties to one side feeling the little hole and you just massaging it pushing your finger on top of it harder and harder

wlldncrazy1: Oh I want you to slide your finger into UC Girl's pussy and get it all nice and wet and then slide your finger in her ass as well

29. wlldncrazy1 also stated "Daddy would pull his panties to one side and take his finger and slide it up his crack until he found the entrance and push slowly and let it slide deep inside of his ass".

30. During the conversations on Kik, wlldncrazy1 provided his username for Wickr, "uralias1957", and stated the OCE should set a Wickr account up for her minor daughter in order for him to talk directly with her because it is more secure and it "burns" or deletes all messages from its server. Wickr is an instant messaging application that allows users to communicate via a secure, encrypted platform, as well as share files, images, and videos.

31. On January 8, 2021, the OCE began communicating with uralias1957, the username provided by wlldncrazy1, on Wickr via an account set up specifically for the adult OCE persona, UC Mom. Additionally, the OCE created a separate Wickr account for the minor daughter persona, UC Girl, and began communicating with uralias1957 from that account as well. The OCE, acting as UC Girl and using the account specifically set up for her persona, sent a message to uralias1957 on Wickr stating, "Hi my mom said I could say hi to you." The conversation between uralias1957 and UC Girl quickly became sexual in nature, including discussion of various sex acts which uralias1957 instructed UC Girl to engage in.

32. The following is an exchange that took place January 13, 2021 between uralias1957 and the

OCE acting as UC Girl:

uralias1957: What are you wearing, have you masturbated today yet ?

UC Girl: Pjs alla time

Nope I dint. U play with ur self?

uralias1957: I did this morning sometime this afternoon you would have to take off your PJs you were just sit in the living room on the couch and you were to masturbate and you were to call UC Boy in so he can sit and watch but he's not allowed to touch.

UC Girl: Y can't he touch me

uralias1957: What did I say

UC Girl: I just don't get y

uralias1957: It's being obedient

UC Girl: K

uralias1957: That's Yes sir

uralias1957: Or yes daddy

33. On January 20, 2021, uralias1957 sent the following messages to UC Girl on Wickr:

uralias1957: What's on your mind what are you thinking about I want you to be able to talk to me about anything and everything

UC Girl: I'm thinking about playing wit u

UC Girl: Mom said she's gunna hold me down but I'll [heart Emoji x 4] it

UC Girl: R we gunna play when I see her

uralias1957: Yes , what do you want to do when play , what do you want

UC Girl: I wanna fuck

UC Girl: Don't u

uralias1957: Daddy is hard

uralias1957: Mmmmm yes

uralias1957: So you ready to feel daddy's dick penetrate and stretch you open , feel it deep in you

uralias1957: So go ahead tell me more tell me all the juicy details that are running through your head right now

34. Later in the conversation, uralias1957 sent the following:

uralias1957: I want you to strip naked in front of me and then pull out daddy's dick and suck it then Daddy's going to finger you and eat your pussy and slide his dick deep inside you and fuck you

uralias1957: Then I'm going to make Mom lick you clean and suck and have UC Boy suck daddy's dick clean

35. Additionally, the following exchange also occurred on the same day:

ralias1957: What more do you want what do you desire how do you feel right now telling Daddy this you're getting daddy's dick hard

UC Girl: I want to ride u like mom used to ride dad

UC Girl: Wut do y want

UC Girl: U

uralias1957: I want to eat your pussy and finger you and suck on your little tiny tits and then I want you to spread your legs wide and Daddy's going to fuck you really deep and you're going to scream and cry because you're going to be in pain but you're going to Buck even harder and want it deeper and then I want you to climb on daddy's dick and I wat you to ride it as often as you want

36. On January 23, 2020, the following messages were exchanged between w1ldncrazy1 and the OCE acting as the adult persona, UC Mom, on Kik:

w1ldncrazy1: I want you naked curled up next to me I'm going to suck on your nipples and finger your clit shove my fingers in your pussy then I'm going to roll over and eat your pussy then have you climb up and suck on Daddy's dick then climb on top of Daddy's dick and ride it then I'm going to bend you over grab you by the back of the hair and Daddy's going to fuck you from behind.

UC Mom: I want you to work me so hard my arms are shaking, struggling to stay up

w1ldncrazy1: Oh yes

w1ldncrazy1: And then we'll call UC Girl in have her come crawl in bed with us

UC Mom: Then what?

w1ldncrazy1: Then I want you to finger her and you eat her pussy and lick her and get her soaking wet and she sucking on Daddy's dick cleaning it off after it's been fucking you then you're to hold her legs wide apart and guide daddy's dick inside of her as he slowly starts pushing further and further in stretching her breaking her in half fucking her deeper and she cries and screams I will not stop

37. Later in the conversation, wlldncrazy1 sent the following message regarding what would happen the first time he met UC Mom in person:

wlldncrazy1: The first time that we meet like you said I want to meet someplace that we can have a drink talk a little bit and get to know each other then go back to your place or I get a motel room and I inspect you from head to toe and I use you for my pleasure for the first time because your number one and your daddy's girl UC Girl will be as well but you get to have the first and she's going to get jealous.

UC Mom: Keeping a little bit for ourselves but sharing it all around

wlldncrazy1: Yes

38. wlldncrazy1 also stated the following, in reference to UC Mom's minor son, "I'm looking forward to being there the very first time UC Boy has an orgasm from either you or UC Girl sucking his dick". In reference to UC Girl, he wrote, "Just wait till I put both of you in the spreader bar and in bondage".

39. Between January 8, 2021 and January 29, 2021, "Dave" continued to communicate with the OCE and discussed plans for him to travel to the Richmond, Virginia area. Dave stated that he planned to arrive in Richmond on or about February 2, 2021 to meet the OCE persona, UC Mom, and, if the meeting is successful, her two minor children. On January 29, 2021, investigators used personally identifiable information from LordWhisper's Alt.com profile, information volunteered during the chat sessions on Alt, Kik, and Wickr, and information obtained from various open source and FBI database queries to identify "Dave" as DAVID HAYES, date of birth (DOB) January 8, 1965, residing in Florence, South Carolina.

40. Since February 2, 2021, HAYES had plans to travel to Richmond, VA several times in order to meet and engage in illegal sexual acts with UC Girl, UC Boy and UC Mom, but his plans were interrupted by health concerns and bad weather.

41. On February 20, 2021, the following messages were exchanged between w1ldncrazy1 and the OCE acting as the adult persona, UC Mom, on Kik regarding what would happen once HAYES arrived in Richmond and had concluded sexual acts with UC Mom:

UC Mom: What would happen after we fuck?

w1ldncrazy1: We would all go climbing your bed and Katie and Tyler can suck on Daddy's dick and clean it off after it's been in your pussy and has all your juices and daddies cum on it

UC Mom: Oh yes

w1ldncrazy1: Daddy fingers Katie's little pussy as I'm sucking on your nipples and biting them

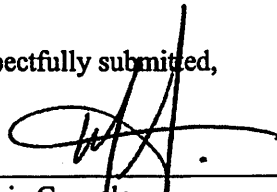
42. On February 26, 2021, HAYES traveled to Richmond Virginia with the intent to engage in illegal sexual acts with a 10-year-old "UC Girl", 8-year-old "UC Boy and their mother "UC Mom". On February 26, 2021, DAVID W. HAYES arrived in the parking lot of the Huguenot Village Shopping Center located on Huguenot Road, Richmond, Virginia. This locations was the meeting spot arranged during conversations between HAYES and the OCE. Law enforcement agents took HAYES into custody at approximately 5:35 PM, once he parked behind a decoy vehicle which the OCE had indicated she would be driving.
43. HAYES was driving the VEHICLE. Agents conducted an onsite security inspection of the vehicle and observed a firearm in the glove compartment, at least two laptops and a phone. Only the firearm was removed from the vehicle and rendered safe prior to placing it in a secured locked storage compartment at the Federal Bureau of Investigation, 1970E Parham Road, Richmond, VA. The VEHICLE was towed to the same location and locked inside the facility. All electronic devices remained inside the vehicle.
44. After HAYES's arrest, he was transported to the Federal Bureau of Investigation, 1970E Parham Road, Richmond, VA. Agents read HAYES his Miranda Rights which he waived and agreed to be interviewed.

45. During the interview HAYES admitted that he used ALT username “**LordWhisper**”, KIK user “**w1ldncrazy1**” and Wickr user “**uralias1957**” and that he was communicating with UC Mom. HAYES advised that he traveled from South Carolina to Virginia to engage in sex with UC Mom but not with the children. When confronted with the extensive amount of online communication where he discussed his plans to engage in illegal sexual acts with UC Mom’s children, HAYES stated that he was only role playing. HAYES also advised that he would have contacted the police and reported UC Mom’s abuse. HAYES also stated that inside the vehicle was his firearm, two computers and his phone. HAYES advised he would not consent to a search of the phone. In addition, HAYES stated that inside the vehicle were gifts for UC Boy and UC Girl and wine. These gifts and the wine are items that were discussed during conversations between UC Mom and HAYES.

CONCLUSION

4 6. Based on the forgoing, I submit that this affidavit supports probable cause for a warrant to search the VEHICLE described in Attachment A for evidence and instrumentalities of violations of Attempted Coercion and Enticement of a Child, in violation of 18 U.S.C. § 2422(b) and Travel With Intent To Engage in Illicit Sexual Conduct with a Child, in violation of 18 U.S.C. § 2423(b), further described in Attachment B.

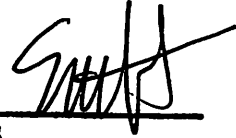
Respectfully submitted,



Melvin Gonzalez
FBI Special Agent

SEEN

_____/s/
Heather Mansfield
Assistant U.S. Attorney

_____/s/ 
Elizabeth W. Hanes
United States Magistrate Judge

Subscribed and sworn to in accordance with
Fed. R. Crim. P. 41 by telephone on March 2 , 2021

ATTACHMENT A

Property to Be Searched

This warrant applies to the VEHICLE described as a 2019 Silver Nissan Pathfinder, VIN 5N1DR2MN9KC643033, with SC license plate SHC863, registered to David HAYES, located at the Federal Bureau of Investigation, 1970E Parham Road, Richmond, VA. (see photographs of the VEHICLE attached below).





ATTACHMENT B

Particular Things to be Seized

1. All records relating to violations of 18 U.S.C. § 2422(b) and Travel With Intent To Engage in Illicit Sexual Conduct with a Child, in violation of 18 U.S.C. § 2423(b) including:
 - a. Any items described during online conversations between OCE and HAYES which would corroborate facts regarding HAYES illegal activities.
 - b. Any and all visual depictions of minors;
 - c. Any and all address books, names and lists of names and addresses of minors;
 - d. Any and all contracts, diaries, notebooks, notes, and other records reflecting physical contacts, whether real or imagined, with minors; and
 - e. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
2. Computers, electronic devices or storage media used as a means to commit the violations described above.
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. Evidence of violations of 18 U.S.C. §§ 2422 and 2423.
 - b. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondences;
 - c. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - d. Evidence of the lack of such malicious software;
 - e. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - f. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER.
 - g. Evidence of the times the COMPUTER was used;
 - h. Passwords, encryption keys, and other access devices that may be necessary to

access the COMPUTER;

- i. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- j. Records of or information about Internet Protocol addresses used by the COMPUTER;
- k. Records of, or information about, the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- l. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in

addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

If the government identifies seized communications to/from an attorney, the investigative team will discontinue review until a filter team of government attorneys and agents is established. The filter team will have no previous or future involvement in the investigation of this matter. The filter team will review all seized communications and segregate communications to/from attorneys, which may or may not be subject to attorney-client privilege. At no time will the filter team advise the investigative team of the substance of any of the communications to/from attorneys. The filter team then will provide all communications that do not involve an attorney to the investigative team and the investigative team may resume its review. If the filter team decides that any of the communications to/from attorneys are not actually privileged (e.g., the communication includes a third party or the crime-fraud exception applies), the filter team must obtain a court order before providing these attorney communications to the investigative team.